JOURNAL OF COMBINATORIAL THEORY, Series A 77, 148–160 (1997)
ARTICLE NO. TA962740

Constructions of Hadamard Difference Sets

Richard M. Wilson and Qing Xiang*

Department of Mathematics, California Institute of Technology, Pasadena, California 91125

Communicated by the Managing Editors

Received May 3, 1996

Using a spread of $PG(3, p)$ and certain projective two-weight codes, we give a general construction of Hadamard difference sets in groups $H \times (Z_p)^4$, where H is either the Klein 4-group or the cyclic group of order 4, and p is an odd prime. In the case $p \equiv 3 \pmod 4$, we use an ovoidal fibration of $PG(3, p)$ to construct Hadamard difference sets, this construction includes Xia's construction of

codes needed in our general construction method. Using a well-known composition theorem, we conclude that there exist Hadamard difference sets with parameters $(4m^2, 2m^2 - m, m^2 - m)$, where $m = 2^a 3^b 5^{2c_1} 13^{2c_2} 17^{2c_3} p_1^2 p_2^2 \cdots p_t^2$ with a, b, c_1, c_2, c_3 positive integers and where each p_j is a prime congruent to 3 modulo 4, $1 \leqslant j \leqslant t$.

1. INTRODUCTION

Let G be a finite group of order v. A k-element subset D of G is called a (v, k, λ) difference set in G if the list of "differences" $d_1 d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$, represents each nonidentity element in G exactly λ times. Using multiplicative notation for the group operation, D is a (v, k, λ) difference set in G if and only if it satisfies the following equation in $Z[G]$,

$$DD^{(-1)} = (k - \lambda)\, 1_G + \lambda G,$$

where $D = \sum_{d \in D} d$, $D^{(-1)} = \sum_{d \in D} d^{-1}$, and 1_G is the identity element of G. D is called reversible if $D^{(-1)} = D$.

In the case G is an abelian group, using the Fourier inversion formula, we have the following standard lemma in the theory of difference sets.

LEMMA A. *Let G be an abelian group of order v. A k-subset D is a (v, k, λ) difference set in G if and only if $|\chi(D)| = \sqrt{k - \lambda}$ for every nontrivial character χ of G. Furthermore, $D = D^{(-1)}$ if and only if $\chi(D) = \overline{\chi(D)}$ for every character χ of G.*

* E-mail: rmw@cco.caltech.edu; xiang@cco.caltech.edu.

0097-3165/97 $25.00

The difference sets considered in this paper have parameters

$$(v, k, \lambda) = (4m^2, 2m^2 - m, m^2 - m).$$

These difference sets are called *Hadamard* difference sets (HDS), since their ± 1 incidence matrices are Hadamard matrices. Alternative names used by other authors are Menon difference sets and H-sets.

The central problem in the study of HDS is for each integer m, which groups of order $4m^2$ contain a Hadamard difference set. This problem remains open, for abelian groups and non-abelian groups as well. However, considerable progress has been made on the construction of Hadamard difference sets in recent years. For example, in 1992, Xia [10] constructed Hadamard difference sets in groups $H \times Z_{p_1}^4 \times Z_{p_2}^4 \times \cdots \times Z_{p_t}^4$, where H is either the Klein 4-group or the cyclic group of order 4, and each p_j is a prime congruent to 3 modulo 4, $1 \leqslant j \leqslant t$. Smith [8] constructed a non-abelian reversible Hadamard difference set in the group $\langle a, b, c \mid a^5 = b^5 = c^4 = [a, b] = cac^{-1}a^{-2} = cbc^{-1}b^{-2} = 1 \rangle$. In October, 1995, Van Eupen and Tonchev [5] constructed a reversible Hadamard difference set in $Z_2 \times Z_2 \times (Z_5)^4$, which is the first example of an abelian Hadamard difference set with the order divisible by a prime congruent to 1 modulo 4.

In this paper, we first give a general construction method for Hadamard difference sets in groups $H \times (Z_p)^4$, where H is either group of order 4 and p is an odd prime, by assuming the existence of certain projective two-weight codes. This method applies to both cases that $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 4$. In section 3, we explain Xia's construction by using our general construction method. This was actually done by Xiang and Chen in [11]. We include this section here for the convenience of the reader. In Section 4, we use an ovoidal fibration of $PG(3, p)$ (see [1, 4, 6]) and spreads associated with it to construct Hadamard difference sets in $H \times (Z_p)^4$, where H is either group of order 4 and p is a prime congruent to 3 modulo 4. This construction includes Xia's construction of Hadamard difference sets as a special case. In Section 5, we explicitly construct those projective two-weight codes needed in our general construction for HDS when $p = 5, 13, 17$. Using a well-known composition theorem of Hadamard difference sets (for example, see [7, 9]), we conclude that there exist Hadamard difference sets with parameters $(4m^2, 2m^2 - m, m^2 - m)$, where $m = 2^a 3^b 5^{2c_1} 13^{2c_2} 17^{2c_3} p_1^2 p_2^2 \cdots p_t^2$ with a, b, c_1, c_2, c_3 positive integers and where each p_j is a prime congruent to 3 modulo 4, $1 \leqslant j \leqslant t$.

2. THE CONSTRUCTION

We begin with the definition of a projective (n, k, h_1, h_2) set in $PG(k-1, q)$, where q is a power of prime p.

DEFINITION. A *projective* (n, k, h_1, h_2) *set* $\mathcal{O}$ is a proper, nonempty set of n points of the projective space $PG(k-1, q)$ with the property that every hyperplane meets $\mathcal{O}$ in h_1 points or h_2 points.

Let $\mathcal{O} = \{\langle y_1\rangle, \langle y_2\rangle, ..., \langle y_n\rangle\}$ be a set of n points in $PG(k-1, q)$. Associated with $PG(k-1, q)$ is the k-dimensional vector space $W = V_k(q)$. Let $\Omega = \{v \in W \mid \langle v\rangle \in \mathcal{O}\}$ be the set of vectors in W corresponding to $\mathcal{O}$. For $w \in GF(q)^k$, define an additive character of $GF(q)^k$ as

$$\chi_w : x \mapsto \xi^{\mathrm{Tr}(w\cdot x)}, \qquad x \in GF(q)^k,$$

where ξ is a primitive pth root of unity and Tr is the trace from $GF(q)$ to $GF(p)$. It is easy to see that χ_w, $w \in GF(q)^k$, are all the additive characters of $GF(q)^k$.

For any nontrivial additive character χ_w of $GF(q)^k$, we have

$$\begin{aligned}\chi_w(\Omega) &= (q-1)|w^\perp \cap \{y_1, y_2, ..., y_n\}| + (-1)(n - |w^\perp \cap \{y_1, y_2, ..., y_n\}|)\\ &= q\,|w^\perp \cap \{y_1, y_2, ..., y_n\}| - n,\end{aligned}$$

where $w^\perp = \{y \in GF(q)^k \mid y \cdot w = 0\}$, and $y \cdot w$ is the usual dot product.

Hence we have the following lemma.

LEMMA 2.1. *$\mathcal{O}$ is a projective (n, k, h_1, h_2) set if and only if $\chi_w(\Omega) = qh_1 - n$ or $qh_2 - n$, for every nontrivial additive character χ_w, $w \in GF(q)^k$.*

Also we mention that projective (n, k, h_1, h_2) sets are equivalent to projective two-weight codes and certain strongly regular Cayley graphs. We refer the reader to the survey papers [3, 7] for more detailed discussion of these three objects.

Let $\Sigma_3 = PG(3, p)$ denote projective 3-space over $GF(p)$, where p is an odd prime. A *spread* of Σ_3 is any collection of p^2+1 pairwise disjoint lines of Σ_3, necessarily partitioning the points of Σ_3. A *partial spread* in Σ_3 is a set of lines no two of which intersect. Also, for convenience, we will call a subset C of Σ_3 *type Q* if C is a projective $((p^4-1)/4(p-1), 4, (p-1)^2/4, (p+1)^2/4)$ set.

THEOREM 2.2. *Assume that $S = \{L_1, L_2, ..., L_{p^2+1}\}$ is a spread of Σ_3. If there exist two subsets C_0, C_1 of type Q in Σ_3 such that $|C_0 \cap L_i| = (p+1)/2$, $1 \leqslant i \leqslant s$, and $|C_1 \cap L_j| = (p+1)/2$, $(s+1) \leqslant j \leqslant 2s$, where $s = (p^2+1)/2$, then there exists a Hadamard difference set in $H \times (Z_p)^4$, where H is either the Klein 4-group or the cyclic group of order 4; in the first case, the Hadamard difference set obtained is reversible.*

Proof. Let $C_2 = (L_1 \cup L_2 \cup \cdots \cup L_s)\backslash C_0$, $C_3 = (L_{s+1} \cup L_{s+2} \cup \cdots \cup L_{2s})\backslash C_1$. We first prove that C_2, C_3 are also two subsets of type Q in Σ_3.

Associated with Σ_3 is the four-dimensional vector space $W = V_4(p)$ over $GF(p)$. Let $\mathscr{C}_0 = \{w \in W \mid \langle w \rangle \in C_0\}$, $\mathscr{C}_2 = \{w \in W \mid \langle w \rangle \in C_2\}$.

Since C_0 is a set of type Q in Σ_3, by Lemma 2.1 we have $\chi(\mathscr{C}_0) = (p^2-1)/4 - p^2$ or $(p^2-1)/4$, for every nontrivial additive character χ of W. We will use W^* to denote the additive character group of W, and define $U = \{\chi \in W^* \mid \chi(\mathscr{C}_0) = (p^2-1)/4 - p^2\}$, $V = \{\chi \in W^* \mid \chi(\mathscr{C}_0) = (p^2-1)/4\}$.

Let $\mathscr{L}_1 = \{w \in W \mid \langle w \rangle \in \bigcup_{i=1}^{s} L_i\}$. Since $\{L_1, L_2, ..., L_s\}$ is a partial spread, we have

$$\chi(\mathscr{L}_1) = \begin{cases} -\dfrac{p^2+1}{2}, & \text{if } \chi \in N_1; \\ \dfrac{p^2-1}{2}, & \text{if } \chi \in T_1, \end{cases}$$

where $N_1 = \{\chi \in W^* \backslash \{\chi_0\} \mid \chi$ is nontrivial on every L_i, $1 \leqslant i \leqslant s\}$ and $T_1 = \{\chi \in W^* \backslash \{\chi_0\} \mid \chi$ is trivial on exactly one L_i for some i, $1 \leqslant i \leqslant s\}$.

We contend that $T_1 \cap U = \varnothing$.

For each L_j, $1 \leqslant j \leqslant 2s$, which is now viewed as a two-dimensional subspace of W, let $L_j^{\perp} = \{\chi \in W^* \mid \chi$ is trivial on $L_j\}$. Then $|L_j^{\perp}| = |W/L_j| = p^2$. For $1 \leqslant j \leqslant s$, we define $\alpha_j = |(L_j^{\perp} \backslash \{\chi_0\}) \cap U|$, $\beta_j = |(L_j^{\perp} \backslash \{\chi_0\}) \cap V|$. Then $\alpha_j + \beta_j = p^2 - 1$.

For every $\chi \in L_j^{\perp}$, we have $\chi(\mathscr{C}_0) = \chi(\mathscr{C}_0 \backslash (\mathscr{C}_0 \cap L_j)) + |\mathscr{C}_0 \cap L_j|$. Therefore,

$$\sum_{\chi \in L_j^{\perp}} \chi(\mathscr{C}_0) = \sum_{w \in \mathscr{C}_0 \backslash (\mathscr{C}_0 \cap L_j)} \; \sum_{\chi \in L_j^{\perp}} \chi(w) + p^2 |\mathscr{C}_0 \cap L_j|.$$

Noting that $\sum_{\chi \in L_j^{\perp}} \chi(w) = 0$ if there is a $\chi \in L_j^{\perp}$ such that $\chi(w) \neq 1$, we have $\sum_{\chi \in L_j^{\perp}} \chi(\mathscr{C}_0) = p^2 |\mathscr{C}_0 \cap L_j|$. That is, $(p^4-1)/4 + \alpha_j((p^2-1)/4 - p^2) + \beta_j(p^2-1)/4 = p^2 |\mathscr{C}_0 \cap L_j|$. Simplifying this we get

$$\frac{1-p^2}{2} + \beta_j = |\mathscr{C}_0 \cap L_j|.$$

Since $|\mathscr{C}_0 \cap L_j| = (p^2-1)/2$ for every j, $1 \leqslant j \leqslant s$, we have $\beta_j = p^2 - 1$, $\alpha_j = 0$, $1 \leqslant j \leqslant s$. Hence, $T_1 \cap U = \varnothing$.

For any nontrivial $\chi \in W^*$, $\chi(\mathscr{C}_2) = \chi(\mathscr{L}_1) - \chi(\mathscr{C}_0)$. Since $T_1 \cap U = \varnothing$, we have

$$\chi(\mathscr{C}_2) = \begin{cases} \dfrac{p^2-1}{4} - p^2, & \text{if } \chi \in N_1 \cap V; \\ \dfrac{p^2-1}{4}, & \text{if } \chi \in (N_1 \cap U) \cup (T_1 \cap V). \end{cases}$$

This shows that C_2 is a set of type Q in Σ_3.

Similarly, define $\mathscr{C}_1 = \{w \in W \mid \langle w \rangle \in C_1\}$, $\mathscr{C}_3 = \{w \in W \mid \langle w \rangle \in C_3\}$. Let $\mathscr{L}_2 = \{w \in W \mid \langle w \rangle \in \bigcup_{i=s+1}^{2s} L_i\}$. Since C_1 is a set of type Q in Σ_3 and $\{L_{s+1}, L_{s+2}, ..., L_{2s}\}$ is a partial spread, we have

$$\chi(\mathscr{C}_1) = \begin{cases} \dfrac{p^2-1}{4} - p^2, & \text{if} \quad \chi \in X, \\ \dfrac{p^2-1}{4}, & \text{if} \quad \chi \in Y, \end{cases}$$

and

$$\chi(\mathscr{L}_2) = \begin{cases} -\dfrac{p^2+1}{2}, & \text{if} \quad \chi \in N_2, \\ \dfrac{p^2-1}{2}, & \text{if} \quad \chi \in T_2, \end{cases}$$

where $N_2 = T_1$ and $T_2 = N_1$.

By the same argument as above, we can show that $T_2 \cap X = \varnothing$; hence,

$$\chi(\mathscr{C}_3) = \begin{cases} \dfrac{p^2-1}{4} - p^2, & \text{if} \quad \chi \in N_2 \cap Y; \\ \dfrac{p^2-1}{4}, & \text{if} \quad \chi \in (N_2 \cap X) \cup (T_2 \cap Y). \end{cases}$$

Assume that A is the union of any $(p^2-1)/4$ lines from $L_{s+1}, L_{s+2}, ..., L_{2s}$, B is the union of any $(p^2-1)/4$ lines from $L_1, L_2, ..., L_s$, and we view A, B as subsets in the vector space W (we make the convention that A, B, when viewed as subsets in W, do not contain the zero vector). Define

$$D_0 = \mathscr{C}_0 \cup A, \qquad D_1 = \mathscr{C}_1 \cup B,$$
$$D_2 = \mathscr{C}_2 \cup A, \qquad D_3 = \mathscr{C}_3 \cup B.$$

For any nontrivial $\chi \in W^*$, we distinguish two cases:

(1) Ker $\chi \supset L_j$, for some j, $1 \leqslant j \leqslant s$. In this case, $\chi \in N_2 = T_1$. Since $T_1 \cap U = \varnothing$, we have $\chi \in V$. Therefore, $\chi(D_0) = (p^2-1)/4 + (-(p^2-1)/4) = 0$, and $\chi(D_2) = (p^2-1)/4 + (-(p^2-1)/4) = 0$,

$$\chi(B) = \begin{cases} p^2 - \dfrac{p^2-1}{4}, & \text{if} \quad L_j \in B; \\ -\dfrac{p^2-1}{4}, & \text{if} \quad L_j \notin B. \end{cases}$$

Hence

$$\chi(D_1)=\begin{cases}0, & \text{if } \chi\in Y;\ L_j\notin B, \text{ or } \chi\in X;\ L_j\in B;\\ \pm p^2, & \text{if } \chi\in Y;\ L_j\in B, \text{ or } \chi\in X;\ L_j\notin B;\end{cases}$$

and

$$\chi(D_3)=\begin{cases}0, & \text{if } \chi\in Y;\ L_j\in B, \text{ or } \chi\in X;\ L_j\notin B;\\ \pm p^2, & \text{if } \chi\in Y;\ L_j\notin B, \text{ or } \chi\in X;\ L_j\in B.\end{cases}$$

This shows that $\chi(D_0)=\chi(D_2)=0$, and only one of $\chi(D_1)$, $\chi(D_3)$ vanishes, the other is $\pm p^2$.

(2) Ker $\chi\supset L_j$, for some j, $(s+1)\leqslant j\leqslant 2s$. In this case, $\chi\in N_1=T_2$. Since $T_2\cap X=\varnothing$, we have $\chi\in Y$. In a manner similar to that of case (1), we can show that $\chi(D_1)=\chi(D_3)=0$ and only one of $\chi(D_0)$, $\chi(D_2)$ vanishes; the other is $\pm p^2$.

We first construct an HDS in the group $Z_2\times Z_2\times(W,+)$. Let us denote the elements of $Z_2\times Z_2$ by $\{1,a,b,ab\}$. Define $D=D_0\cup aD_1\cup bD_2\cup ab(W\backslash D_3)$. We contend that D is a reversible Hadamard difference set in $Z_2\times Z_2\times(W,+)$.

Let $\phi\otimes\chi$ be an arbitrary nontrivial character of $Z_2\times Z_2\times W$.

If χ is trivial, ϕ is nontrivial, then

$$\phi\otimes\chi(D)=|D_0|+\phi(a)|D_1|+\phi(b)|D_2|+\phi(ab)|W\backslash D_3|=p^2\phi(ab),$$

so $|\phi\otimes\chi(D)|=p^2$.

If χ is nontrivial, by the discussion in the two cases above, we have

$$\phi\otimes\chi(D)=\pm p^2;$$

hence $|\phi\otimes\chi(D)|=p^2$.

By Lemma A, D is a Hadamard difference set. Since $\psi(D)=\overline{\psi(D)}$ for every nontrivial character ψ of $Z_2\times Z_2\times W$, D is reversible. In the case the group is $Z_4\times(Z_p)^4$, let the elements of Z_4 be $\{1,c,c^2,c^3\}$, and $D=D_0\cup cD_1\cup c^2D_2\cup c^3(W\backslash D_3)$. Then it is easy to show that D is a Hadamard difference set in $Z_4\times(W,+)$. This completes the proof of the theorem. ∎

3. ON XIA'S CONSTRUCTION

In 1992, Xia [10] constructed Hadamard difference sets in groups $H\times Z_{p_1}^4\times Z_{p_2}^4\times\cdots\times Z_{p_t}^4$, where H is either group of order 4 and each p_j is a prime congruent to 3 modulo 4, $1\leqslant j\leqslant t$. Xia's construction depends on

very complicated calculations involving cyclotomic classes of high order. Xiang and Chen [11] have given a simpler proof for Xia's construction by using additive characters of finite fields.

In view of Theorem 2.2, in order to construct Hadamard difference sets in $H \times (Z_p)^4$, where H is either group of order 4 and p is a prime congruent to 3 modulo 4, all we need are a spread in Σ_3, and sets C_0, C_1 of type Q in Σ_3 satisfying the conditions in Theorem 2.2.

Let p be a prime congruent to 3 modulo 4 and let β be a primitive element of $GF(p^4)$. We model Σ_3 by viewing $GF(p^4)$ as four-dimensional vector space over $GF(p)$. Thus the points of Σ_3 are represented by $\langle 1 \rangle$, $\langle \beta \rangle$, ..., $\langle \beta^{(p^2+1)(p+1)-1} \rangle$. Let $L_i = \{\langle \beta^i \rangle, \langle \beta^{(p^2+1)+i} \rangle, ..., \langle \beta^{p(p^2+1)+i} \rangle\}$, $0 \leqslant i \leqslant p^2$. Then it is easy to see that $S = \{L_0, L_1, ..., L_{p^2}\}$ is a spread in Σ_3. Let $C_0 = \{\langle 1 \rangle, \langle \beta^4 \rangle, \langle \beta^8 \rangle, ..., \langle \beta^{(p^2+1)(p+1)-4} \rangle\}$, $C_1 = \{\langle \beta \rangle, \langle \beta^5 \rangle, \langle \beta^9 \rangle, ..., \langle \beta^{(p^2+1)(p+1)-3} \rangle\}$. Since $p \equiv 3 \pmod 4$, by uniform cyclotomy (see [2, 7]), C_0, C_1 are two sets of type Q in Σ_3. Also it is easy to see that $|C_0 \cap L_{2i}| = (p+1)/2$, $0 \leqslant i \leqslant (p^2-1)/2$, and $|C_1 \cap L_{2i+1}| = (p+1)/2$, $0 \leqslant i \leqslant (p^2-1)/2$. Therefore by Theorem 2.2, we have

COROLLARY 3.1. *There exists a Hadamard difference set in* $H \times (Z_p)^4$, *where* p *is a prime congruent to* 3 *modulo* 4 *and* H *is either the Klein* 4*-group or the cyclic group of order* 4. *In the first case, the Hadamard difference set constructed by Theorem* 2.2 *is reversible.*

Using a composition theorem of Turyn [9], it is routine to construct Hadamard difference sets in $H \times Z_{p_1}^4 \times Z_{p_2}^4 \times \cdots \times Z_{p_t}^4$, where H is either group of order 4, and each p_j is a prime congruent to 3 modulo 4, $1 \leqslant j \leqslant t$.

4. GENERAL CONSTRUCTION IN THE CASE $p \equiv 3 \pmod 4$

In this section, we give a general construction of Hadamard difference sets in $H \times (Z_p)^4$, where H is either group of order 4, and p is a prime congruent to 3 modulo 4, by using an ovoidal fibration of $PG(3, p)$ in [1, 4, and 6, page 253]. We introduce the following notation as in [1, 4].

Let p be a prime congruent to 3 modulo 4. We view $GF(p^4)$ as a four-dimensional vector space over $GF(p)$, and, hence, the one-dimensional subspaces of this vector space can be thought of as the projective points of $\Sigma_3 = PG(3, p)$. Similarly, we identify the lines of Σ_3 with the two-dimensional vector subspaces of $GF(p^4)$ over $GF(p)$. We also let $\langle A \rangle$ denote the vector subspace generated by the set A over $GF(p)$.

If β is a primitive element of $GF(p^4)$, then $o(\beta) = p^4 - 1 = (p+1)(p-1)(p^2+1)$ and hence $\beta^{(p+1)(p^2+1)}$ is a primitive element of

$GF(p)$. We therefore identify the points of Σ_3 with $\{\langle\beta^t\rangle \mid t=0, 1, 2, ..., (p+1)(p^2+1)-1\}$. If we now let $\Omega_i=\{\langle\beta^t\rangle \mid t\equiv i \pmod{p+1}\}$, each Ω_i is an ovoid (Theorem 3 of [4]) and the points of Σ_3 are thus partitioned into $p+1$ disjoint ovoids:

$$\Sigma_3=\Omega_0\cup\Omega_1\cup\cdots\cup\Omega_p. \qquad (*)$$

Moreover, each line of Σ_3 is tangent to precisely 0 or 2 of these ovoids (Lemma 1 and Theorem 4 of [4]). Lines of the former type will be called "secant-type" and those of the latter "tangent-type". If $L_s=\langle\beta^0, \beta^{s(p+1)}\rangle$ denotes the line of Σ_3 joining the points $\langle\beta^0\rangle$ and $\langle\beta^{s(p+1)}\rangle$ of Ω_0 for any integer s with $1\leqslant s\leqslant p^2$, then L_s is a secant-type line if and only if s is odd (Theorem 4 of [4]).

If L is any line of Σ_3, let $[L]$ denote the line orbit of L under the collineation of Σ_3 corresponding to multiplication by $\beta^{2(p+1)}$. Also let L^p denote the image of the line L under the collineation corresponding to the Frobenius automorphism, and let $L\beta^d$ denote the image of L under multiplication by β^d.

We quote the following theorem and corollary from [1].

THEOREM B. *Using the above notation, let s be an odd integer with $1\leqslant s\leqslant p^2$. Consider the secant-type line $L_s=\langle\beta^0, \beta^{s(p+1)}\rangle$, necessarily secant to $(p+1)/2$ ovoids in the fibration $(*)$. Then there exists a positive integer d such that $(L_s)^p\beta^d$ is a secant-type line meeting the $(p+1)/2$ ovoids of $(*)$ missed by L_s. Moreover, if $s\neq(p^2+1)/2$, d is unique modulo $p+1$.*

COROLLARY C. *$[L_s]\cup[(L_s)^p\beta^d]$ is a spread of Σ_3. This spread is regular precisely when $s=(p^2+1)/2$.*

Now we use the spread in Corollary C to construct Hadamard difference sets. By Theorem 2.2, we need to come up with two sets C_0, C_1 in Σ_3 of type Q satisfying the conditions in Theorem 2.2.

Let L_s and $(L_s)^p\beta^d$ be the secant-type lines in Theorem B. We assume that L_s is secant to Ω_{t_1}, Ω_{t_2}, ..., Ω_{t_r}, and $(L_s)^p\beta^d$ is secant to $\Omega_{t_{r+1}}$, $\Omega_{t_{r+2}}$, ..., $\Omega_{t_{2r}}$, where $r=(p+1)/2$. By Theorem B, $\{t_1, t_2, ..., t_{2r}\}=\{0, 1, 2, ..., p\}$. Since $p\equiv 3 \pmod 4$, r is even. Let C_0 be the union of any $r/2$ ovoids from $\{\Omega_{t_1}, \Omega_{t_2}, ..., \Omega_{t_r}\}$, and let C_1 be the union of any $r/2$ ovoids from $\{\Omega_{t_{r+1}}, \Omega_{t_{r+2}}, ..., \Omega_{t_{2r}}\}$. Then we have the following lemma.

LEMMA 4.1. *C_0 meets every line in $[L_s]$ in $(p+1)/2$ points, and C_1 meets every line in $[(L_s)^p\beta^d]$ in $(p+1)/2$ points. C_0, C_1 are two sets of type Q in Σ_3.*

Proof. The first assertion is clear by the definition of C_0 and C_1. For the proof of the second part, we observe that every plane of Σ_3 must meet each of the $p+1$ ovoids in $(*)$ in a point or an oval. A simple counting argument then shows that each plane of Σ_3 is tangent to 1 of the ovoids in $(*)$ and meets the other p ovoids in disjoint ovals. Let π be an arbitrary plane of Σ_3. Then $|\pi \cap C_0| = 1 + (r/2-1)(p+1) = (p-1)^2/4$ if C_0 contains some Ω_{t_j} such that $|\pi \cap \Omega_{t_j}| = 1$, $1 \leqslant j \leqslant r$, and $|\pi \cap C_0| = (r/2)(p+1) = (p+1)^2/4$ if $|\pi \cap \Omega_{t_i}| = p+1$ for every Ω_{t_i} contained in C_0. This shows that C_0 is a set of type Q in Σ_3. Similarly, we can show that C_1 is also a set of type Q in Σ_3. This completes the proof of the lemma. ∎

COROLLARY 4.2. *Let* $[L_s] \cup [(L_s)^p \beta^d]$, C_0, C_1 *be defined as above. Then there exists a Hadamard difference set in* $H \times (Z_p)^4$, *where* H *is either group of order* 4, *and* p *is a prime congruent to* 3 *modulo* 4, *by using the spread* $[L_s] \cup [(L_s)^p \beta^d]$ *and the sets* C_0 *and* C_1 *of type Q in* Σ_3.

Proof. This is clear from Lemma 4.1 and Theorem 2.2. ∎

Remarks. (1) If we let $s = (p^2+1)/2$, then $L_s = GF(p^2)$, $L_s^p = L_s$, and $[L_s] \cup [\beta L_s]$ is the regular spread in Section 3. Also we note that L_s meets the ovoids Ω_0, Ω_2, Ω_4, ..., Ω_{p-1} (Lemma 1 of [4]), and βL_s meets the ovoids Ω_1, Ω_3, Ω_5, ..., Ω_p. If we choose the union of Ω_0, Ω_4, Ω_8, ..., Ω_{p-3} as C_0 and the union of Ω_1, Ω_5, Ω_9, ..., Ω_{p-2} as C_1, then the construction in this section will give rise to Xia's construction.

(2) Let $G = K_4 \times P$, where K_4 is the Klein 4-group and $P = Z_p^4$, p is a prime congruent to 3 modulo 4. Two difference sets D and D' in G are said to be equivalent if $D' = gD^\alpha$ for some automorphism α of G and some element g of G. Since K_4 and P have relatively prime orders, they must be invariant under every automorphism of G. Therefore the automorphism group of G has size $|GL(2, 2)|\,|GL(4, p)| = 6p^6(p^4-1)(p^3-1)(p^2-1)(p-1)$. From Theorem 2.2 and the construction in this section, we see that there are at least

$$\frac{4!\,\dfrac{p^2+1}{2}\dbinom{(p+1)/2}{(p+1)/4}^2\dbinom{(p^2+1)/2}{(p^2-1)/4}^2}{4p^4 \cdot 6p^6(p^4-1)(p^3-1)(p^2-1)(p-1)}$$

$$= \frac{(p^2+1)\dbinom{(p+1)/2}{(p+1)/4}^2\dbinom{(p^2+1)/2}{(p^2-1)/4}^2}{2p^{10}(p^4-1)(p^3-1)(p^2-1)(p-1)}$$

pairwise inequivalent Hadamard difference sets in G.

5. THE CASE $p \equiv 1 \pmod 4$

In this section, we construct sets of type Q in $\Sigma_3 = PG(3, p)$ with $p \equiv 1 \pmod 4$. Again let W be the four-dimensional vector space over $GF(p)$ associated with Σ_3. We may consider W as a direct product $GF(p^2) \times GF(p^2)$.

Let g be a primitive element of $GF(p^2)$. L_∞ will denote the line $\{0\} \times GF(p^2)$, and for any d in $GF(p^2)$, L_d will denote the line $\{(x, dx^p) \mid x \in GF(p^2)\}$. It is easy to verify that $S = \{L_d \mid d \in GF(p^2)\} \cup \{L_\infty\}$ is a spread in Σ_3.

We now consider the action of

$$T = \begin{pmatrix} g^2 & 0 \\ 0 & g^{-2} \end{pmatrix}$$

on the points of Σ_3 which are now viewed as one-dimensional subspaces over $GF(p)$ of the four-dimensional vector space $GF(p^2) \times GF(p^2)$ over $GF(p)$.

The orbits of the action of T on the points of Σ_3 are

(1) Four "short" orbits, each of length $(p+1)/2$. We choose $(0, 1)$, $(0, g)$, $(1, 0)$, and $(g, 0)$ as the representatives of these four orbits.

(2). $4(p+1)$ "long" orbits, each of length $(p^2-1)/4$. The representatives of these $4(p+1)$ orbits can be chosen as

$$(1, 1), (1, g), (1, g^2), ..., (1, g^{2p+1}),$$
$$(g, 1), (g, g), (g, g^2), ..., (g, g^{2p+1}).$$

It is clear that each short orbit consists of $(p+1)/2$ points of L_0 or L_∞.

Next we show that each long orbit consists of $(p+1)/2$ points of $(p-1)/2$ lines from the set of lines $\{L_d \mid d \neq 0,\ d \in GF(p^2)\}$. For example, take the long orbit represented by $(1, g^i)$, $0 \leqslant i \leqslant 2p+1$. Let $a = g^i$. The points in this orbit are represented by

$$(1, a) \to \quad (g^2, ag^{-2}) \quad \to \cdots \to \quad (g^{p-3}, ag^{3-p}) \to$$
$$(g^{p-1}, ag^{1-p}) \to (g^{p+1}, ag^{-1-p}) \to \cdots \to \quad (g^{2p-4}, ag^{4-2p}) \to$$
$$\cdots$$
$$(g^l, ag^{-l}) \to (g^{l+2}, ag^{-l-2}) \to \cdots \to (g^{l+p-3}, ag^{-l-p+3}),$$

where $l = (p-1)^2/2$. Each column in the above diagram consists of $(p+1)/2$ points of some line L_d, $d \neq 0$, $d \in GF(p^2)$; hence the orbit represented by $(1, g^i)$ consists of $(p+1)/2$ points of $(p-1)/2$ lines from the

set of lines L_d, $d \neq 0$, $d \in GF(p^2)$. This argument applies to any orbit represented by (g, g^i), $0 \leqslant i \leqslant 2p+1$.

For $p=5$ let g be a root of $x^2+x+2 \in GF(5)[x]$. With the help of a computer (we will give more details about the computer search at the end of this section), we found that the union of the following orbits

$$(1, g), (1, g^2), (1, g^9), (1, g^{11}), (g, 1), (g, g^8), (1, 0)$$

forms a set of type Q in $PG(3, 5)$, which we will call C_0, also the union of the following orbits

$$(1, g^6), (1, g^8), (1, g^{10}), (g, g^5), (g, g^9), (g, g^{10}), (0, 1)$$

forms another set of type Q in $PG(3, 5)$, which we denote by C_1. Let $S = \{L_d \mid d \in GF(5^2)\} \cup \{L_\infty\}$. We have seen that each orbit of T intersects the lines in S in 0 or 3 points, also no two orbits of T in C_0, C_1 intersect the same line, hence C_0, C_1 satisfy the conditions of Theorem 2.2. Therefore there exists a Hadamard difference set in $H \times (Z_5)^4$, where H is either group of order 4. We state this as a corollary.

COROLLARY 5.1. *There exists a Hadamard difference set in* $H \times (Z_5)^4$, *where H is either the Klein* 4*-group or the cyclic group of order* 4; *in the first case, the Hadamard difference set is reversible.*

Remark. Van Eupen and Tonchev ([5]) were the first to construct a reversible Hadamard difference set in $Z_2 \times Z_2 \times (Z_5)^4$. We remark that the structure of the Hadamard difference set in $Z_2 \times Z_2 \times (Z_5)^4$ constructed in Corollary 5.1 is different from that of Van Eupen and Tonchev's Hadamard difference set. For example, in Theorem 2.2 (hence in Corollary 5.1), we choose A, B both as union of lines from a spread in Σ_3, while in Van Eupen and Tonchev's example, one projective (36, 4, 6, 11) set in $PG(3, 5)$ comes from the union of six lines, the other does not.

In the case $p=13$, let g be a root of $x^2+x+2 \in GF(13)[x]$. With the help of a computer, we found the following two sets of type Q in $PG(3, 13)$.

The union of the orbits

$$(1, g^5), (1, g^6), (1, g^9), (1, g^{13}), (1, g^{15}), (1, g^{17}), (1, g^{18}), (1, g^{24}),$$
$$(g, g^4), (g, g^5), (g, g^8), (g, g^{14}), (g, g^{16}), (g, g^{23}), (1, 0)$$

forms a set of type Q in $PG(3, 13)$, which we will denote by C_0. And the union of the orbits

$$(1, 1), (1, g^2), (1, g^4), (1, g^7), (1, g^8), (1, g^{12}), (1, g^{25}), (g, g), (g, g^6),$$
$$(g, g^7), (g, g^{11}), (g, g^{12}), (g, g^{24}), (g, g^{27}), (0, 1)$$

forms another set of type Q, which we will denote by C_1. Let $S = \{L_d \mid d \in GF(13^2)\} \cup \{L_\infty\}$. It is easy to see that S, C_0, C_1 satisfy the conditions in Theorem 2.2.

By Theorem 2.2, we have

COROLLARY 5.2. *There exists a Hadamard difference set in* $H \times (Z_{13})^4$, *where* H *is either the Klein* 4*-group or the cyclic group of order* 4; *in the first case the Hadamard difference set is reversible.*

When $p = 17$, let g be a root of $x^2 + x + 3 \in GF(17)[x]$. With the help of a computer, we found the following two sets of type Q in $PG(3, 17)$. The union of the orbits

$$(1, g^2), (g, g), (1, g^7), (g, g^6), (1, g^{12}), (g, g^{11}), (1, g^{15}),$$
$$(g, g^{14}), (1, g^{19}), (g, g^{18}), (1, g^{26}), (g, g^{25}), (1, g^{32}), (g, g^{31}), (1, g^{34}),$$
$$(g, g^{33}), (1, g^{21}), (1, g^{22}), (1, 0)$$

forms a set of type Q in $PG(3, 17)$, which we will denote by C_0. And the union of the following orbits

$$(1, g^5), (g, g^4), (1, g^6), (g, g^5), (1, g^9), (g, g^8), (1, g^{10}),$$
$$(g, g^9), (1, g^{11}), (g, g^{10}), (1, g^{17}), (g, g^{16}), (1, g^{18}), (g, g^{17}), (1, g^{31}),$$
$$(g, g^{30}), (1, g^4), (g, g^{20}), (0, 1)$$

forms another set of type Q in $PG(3, 17)$, which we will denote by C_1. Let $S = \{L_d \mid d \in GF(17^2)\} \cup \{L_\infty\}$. Then it is easy to check that S, C_0, C_1 satisfy the conditions in Theorem 2.2.

By Theorem 2.2, we have

COROLLARY 5.3. *There exists a Hadamard difference set in* $H \times (Z_{17})^4$, *where* H *is either the Klein* 4*-group or the cyclic group of order* 4; *in the first case, the Hadamard difference set is reversible.*

Remark. We give more details about our computer search in what follows. In order to search for sets of type Q in Σ_3 by computer, we first noted that T also permutes the planes in four "short" orbits and $4(p+1)$ "long" orbits. We formed a square nonnegative integral matrix M whose rows were indexed by the orbits of T on the points, whose columns were indexed by the orbits of T on the planes, and where the entry in row i and column j was the the cardinality of the intersection of a (any) plane in plane-orbit j with the ith orbit of points. A union of point-orbits is a set of type Q if and only if the sum of the corresponding rows of M has entries $(p \pm 1)^2/4$ only.

For example, when $p = 17$, the matrix M is square of order 76. The sum of all rows was a constant vector of 307s. We searched for 19 rows (one row corresponding to a short orbit and the others to long orbits) so that the sum of the 19 rows had entries 64 and 81 only. Our search was not exhaustive but simply moved from one set of 19 rows to another set by deleting one row—with a large entry in a column where the sum exceeded 81—and randomly adding another one. This was done with Mathematica on a PC.

Finally, using a composition theorem of Turyn [9], it is routine to construct $(4m^2,\ 2m^2-m,\ m^2-m)$ Hadamard difference sets with $m = 2^a 3^b 5^{2c_1} 13^{2c_2} 17^{2c_3} p_1^2 p_2^2 \cdots p_t^2$, where a, b, c_1, c_2, c_3 are positive integers and each p_j is a prime congruent to 3 modulo 4, $1 \leqslant j \leqslant t$.

ACKNOWLEDGMENTS

We thank G. Ebert, W. Kantor, and V. Tonchev for their helpful discussions.

REFERENCES

1. R. D. Baker and G. L. Ebert, Construction of two-dimensional flag-transitive planes, *Geom. Dedicata* **27** (1988), 9–14.
2. L. D. Baumert, W. H. Mills, and R. L. Ward, Uniform cyclotomy, *J. Number Theory* **14** (1982), 67–82.
3. A. R. Calderbank and W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.* **18** (1986), 97–122.
4. G. L. Ebert, Partitioning projective geometries into caps, *Canad. J. Math.* **37**, No. 6 (1988), 1163–1175.
5. M. van Eupen and V. D. Tonchev, The existence of a reversible Hadamard difference set in $Z_2 \times Z_2 \times (Z_5)^4$ and an infinite class of Williamson matrices, preprint, Oct. 1995.
6. J. H. van Lint and R. M. Wilson, "A Course in Combinatorics," Cambridge Univ. Press, Cambridge, 1992.
7. S. L. Ma, A survey of partial difference sets, *Designs, Codes, Cryptogr.* **4** (1994), 221–261.
8. K. W. Smith, Non-abelian Hadamard difference sets, *J. Combin. Theory Ser. A* **70** (1995), 144–156.
9. R. J. Turyn, A special class of Williamson matrices and difference sets, *J. Combin. Theory Ser. A* **36** (1984), 111–115.
10. M. Y. Xia, Some infinite classes of special Williamson matrices and difference sets, *J. Combin. Theory Ser. A* **61** (1992), 230–242.
11. Q. Xiang and Y. Q. Chen, On Xia's construction of Hadamard difference sets, *Finite Fields Appl.* **2** (1996), 87–95.